REMARKS

The Examiner has rejected Claims 1-11, 17, 19-23, 25-29, and 35 under 35 U.S.C. 103(a) as being unpatentable over Chess et al. (U.S. 6,560,632) in further in view of Wong (U.S. 5,974,465). Further, the Examiner has rejected Claims 37-41, and 43-53 under 35 U.S.C. 103(a) as being unpatentable over Chess et al. (U.S. 6,560,632), further in view of Wong (U.S. 5,974,465), and further in view of Chiussi et al. (U.S. 6,532,213). Still yet, the Examiner has rejected Claims 55-59 under 35 U.S.C. 103(a) as being unpatentable over Chess et al. (U.S. 6,560,632), further in view of Wong (U.S. 5,974,465), further in view of Chiussi et al. (U.S. 6,532,213), further in view of "Chapter Thirteen Performance Tuning," and further in view of Using NetWare 3.12. Applicant respectfully disagrees with these rejections.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991). Applicant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met.

With respect to the first element of the *prima facie* case of obviousness, the Examiner states that it would have been obvious to one of ordinary skill in the art at the time of the invention was made to use Wong's method of prioritization to prioritize the requests of Chess et al. Applicant respectfully disagrees with this proposition, especially in view of the vast evidence to the contrary.

For example, Chess relates to a distributed security system, while Wong relates to a network data packet prioritization system. To simply glean features from a network data packet

prioritization system, such as that of Wong, and combine the same with the *non-analogous art* of distributed security systems, such as that of Chess would simply be improper. A network data packet prioritization system prioritizes data packets via a network device, while a distributed security system detects viruses, etc. "In order to rely on a reference as a basis for rejection of an applicant's invention, the reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the inventor was concerned." In re Oetiker, 977 F.2d 1443, 1446, 24 USPQ2d 1443, 1445 (Fed. Cir. 1992). See also In re Deminski, 796 F.2d 436, 230 USPQ 313 (Fed. Cir. 1986); In re Clay, 966 F.2d 656, 659, 23 USPQ2d 1058, 1060-61 (Fed. Cir. 1992) In view of the vastly different types of problems a distributed security system addresses as opposed to a network data packet prioritization system, the Examiner's proposed combination is inappropriate. To simply dismiss applicant's unique application of prioritization techniques in the specific context of a security system would improperly frustrate the inventive concepts of applicant.

With respect to the third element of the *prima facie* case of obviousness, the Examiner relies on the following excerpt from Chess to meet applicant's claimed: "checking a virus scan request to determine if scanning an object of the request is necessary; and placing the virus scan request on a queue in a priority order based on a characteristic of the virus scan request" (see Claim 1 and similar, but not identical, language in remaining independent claims).

> "The units of digital data preferably include queries or files. In one such embodiment, the distributed system includes a computer protection system and the units of digital data include files or checksums of files which are suspected to contain malicious code. The malicious code may include computer viruses, worms or Trojan Horses.
>
> It is preferable that the prioritizing step comprises the steps of: classifying the queued queries or files into categories, clustering the files, in each of the categories, into similarity clusters; choosing, for each similarity cluster, one or more representatives; and determining an order of processing for the one or more representatives. The classifying step preferably includes the step of classifying the queued queries or files according to the type of digital object they contain." (col. 3, lines 42-56)

Applicant respectfully disagrees with this assertion. Specifically, Chess merely suggests classifying queries or files *already* queued, for *prioritized processing*. In sharp contrast, applicant teaches and claims placing the virus scan requests on a queue in a priority order based

on a characteristic of the virus scan request, for *prioritized queuing*. Thus, Chess's prioritization (as well as Wong's, for that matter) is specific to a *classification* process that occurs *after queuing*, while applicant's prioritization is specific to the *queuing process* itself *during queuing*.

Still yet, the Examiner relies on the following excerpt from Wong to meet applicant's claimed: "the characteristic including at least one of an identity of the user triggering the virus scan request ... wherein the virus scan request is prioritized based on at least one of the user identity being an administrator as compared to a regular user" (see Claim 1 and similar, but not identical, language in remaining independent claims).

> "Whenever an outbound packet is to be transmitted, prioritization software module 208 examines that packet to determine whether it should be stored in queue 209. The prioritization software module 208 makes its determination based upon a particular configuration scheme. It is the function of software module 208 to initially configure the prioritization scheme. The configuration process entails specifying a number of different priority levels. For each of these priority levels, the software module 208 specifies a number of buffers within queue 209 which are to be reserved for that particular priority level. A buffer is a discrete unit of memory which is used to store one packet. The size of the packets and buffers can vary, depending on the hardware and software considerations." (col. 4, lines 14-41)

Applicant respectfully disagrees with this assertion. Specifically, there is absolutely no mention in the foregoing excerpt, nor the remaining Wong reference, of any sort of placing virus scan requests in a queue based on a virus scan request characteristic including "an identity of the user triggering the virus scan request ... wherein the virus scan request is prioritized based on at least one of the user identity being an administrator as compared to a regular user" (emphasis added), as claimed.

Applicant thus respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. A notice of allowance or a specific prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

With respect to Claim 37, the Examiner relies on the following excerpt from Chiussi to meet applicant's claimed "the characteristic including ... a time stamp of when the virus request was received ... wherein the virus scan request is prioritized based on ... the time stamp being earlier than the time stamps of each scan request previously placed on the queue" (see Claim 1 and similar, but not identical, language in remaining independent claims).

> "A system is disclosed that services a plurality of queues associated with respective data connections in a packet communication network such that the system guarantees data transfer delays between the data source and the destination of each data connection. This is achieved in two stages. The first stage shapes the traffic of each connection such that it conforms to a specified envelope. The second stage associates timestamps with the packets released by the first stage and chooses for transmission from among them the one with the smallest timestamp. Both stages are associated with a discrete set of delay classes. The first stage employs one shaping structure per delay class. Each shaping structure in turn supports a discrete set of rates and employs a FIFO of connections per supported rate. A connection may move between FIFOs corresponding to different rates as its rate requirement changes. The second stage associates with each packet exiting the first stage a timestamp given by the exit time from the first stage and the delay class to which the connection belongs. A queue of packets is maintained per delay class, and the scheduler selects for transmission from among the packets at the head of the queues the one with the smallest timestamp." (Abstract)

Applicant respectfully disagrees with this assertion. Specifically, there is absolutely no mention in the foregoing excerpt, nor the remaining Chiussi reference, of any sort of placing virus scan requests in a queue based on a virus scan request characteristic including "a time stamp of when the virus request was received ... wherein the virus scan request is prioritized based on ... the time stamp being earlier than the time stamps of each scan request previously placed on the queue" (emphasis added), as claimed.

Moreover, with respect to Claim 55, the Examiner relies on the following excerpts from Performance and NetWare to meet applicant's claimed "the characteristic including .... a type of the process accessing the object... and an indication of a network node accessing the object, wherein the virus scan request is prioritized based on .... the process type being an operating system as compared to a user applicant and ..... the indication being that the object is accessed from a server console as compared to a network client" (see Claim 1 and similar, but not identical, language in remaining independent claims).

Application Priority

- 0-15: User-accessible process priorities
  - 0-6: Low user range
  - 4: Low value
  - 7: Normal
  - 13: High value
  - 8-15: High user range
- 16-31: System-accessible process priorities
  - 16-24: Real-time values accessible to Administrator-level accounts
  - 24: Real-time value
  - 25-31: Real-time value accessible to operating system only

(see page 4 of Performance)

SEND

SEND is used almost exactly like BROADCAST. The only difference is that messages sent with SEND are treated as regular-priority messages, similar to those you receive from another user's workstation, whereas messages sent with BROADCAST are treated as high-priority alerts from the server console. Users can prevent receipt of messages sent with SEND by using the CASTOFF command, but BROADCAST requires the CASTOFF ALL command.

(see page 7 of Netware)

In the Examiner's latest response to arguments, the Examiner argues that "Performance teaches prioritization based on process types (see page 4) and Netware teaches prioritization based on network node type (see page 8)." Applicant respectfully disagrees with such assertion, as it appears that the Examiner has simply failed to consider the full weight of applicant's claims.

Specifically, the Performance excerpt above simply fails to meet applicant's claimed "characteristic including .... a type of the process accessing the object... wherein the virus scan request is prioritized based on .... the process type being an operating system as compared to a user application" (emphasis added). As clearly set forth in the relevant excerpts hereinabove, Performance suggests processes that are accessible by user and system applications, and fall short of a process that specifically accesses the object, as claimed, where one of the process types is an operation system process (note that a system application does not meet an operating system).

Further, the Netware excerpt above fails to meet applicant's claimed "characteristic including ....an indication of a network node accessing the object, wherein the virus scan request is prioritized based on ... the indication being that the object is accessed from a server console as compared to a network client." Again, similar to the Performance reference, Netware does not meet applicant's claimed node that accesses the object, as claimed. Instead Network merely suggests two types of messages, one sent using a SEND feature, and one sent using a BROADCAST feature.

Again, a notice of allowance or a specific prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

To this end, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

Reconsideration is respectfully requested.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. Applicants are enclosing a check to pay for the added claims. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P360).

Respectfully submitted,
Zilka-Kotab, PC

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100